THE FBI FEDERAL BUREAU OF INVESTIGATION

Testimony

Robert S. Mueller, III
Director
Federal Bureau of Investigation

United States Senate Committee on the Judiciary Sunset Provisions of the USA Patriot Act
Washington, DC

April 05, 2005

Good morning Mr. Chairman, Senator Leahy and Members of the Committee. I am pleased to be here today with the Attorney General to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its efforts in the war on terror. For almost three and a half years, the USA Patriot Act has changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act. As you know, several of these provisions are scheduled to "sunset" at the end of this year. I firmly believe that it is crucial to our national security to renew these provisions. Without them, the FBI might well be forced into pre-September 11th practices, requiring us - agents, analysts and our partners - to fight the war on terror with one hand tied behind our backs.

USA Patriot Act SUNSET PROVISIONS

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing).

Section 201 brought the federal wiretap statute into the 21st century. Prior to its passage, law enforcement was not authorized to conduct electronic surveillance when investigating crimes committed by terrorists, such as chemical weapons offenses, killing U.S. nationals abroad, using weapons of mass destruction, and providing material support to terrorist organizations. Section 201 closed an existing gap in the Title III statute. Now Agents are able to gather information when looking into the full range of terrorism related crimes.

Similarly, Section 202 brought the criminal code up to date with modern technology by adding felony offenses under the Computer Fraud and Abuse Act, such as computer espionage, extortion and intentionally damaging a federal government computer, to the list of wiretap predicates in 18 U.S.C. §2516(1). This provision eliminated an anomaly in the law and now permits Agents to obtain wiretap orders to monitor wire and oral communications to investigate serious computer crimes.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. If Section 203(b) were allowed to expire, FBI Agents would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, but would arguably not be allowed to share that same information with the CIA. This result would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to

Recent Testimonies

03.27.14 **FBI Budget Request for Fiscal Year 2015**
James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C.

03.26.14 **FBI Budget Request for Fiscal Year 2015**
James B. Comey, Director, Federal Bureau of Investigation, Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C.

03.26.14 **Innocence for Sale: Domestic Minor Sex Trafficking**
Michael T. Harpster, Acting Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, Washington, D.C.

11.14.13 **Cartel Prosecution: Stopping Price Fixers and Protecting Consumers**
Ronald T. Hosko, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Joint Statement with Antitrust Division Assistant Attorney General William J. Baer Before the Senate Judiciary Committee, Subcommittee on Antitrust, Competition Policy, and Consumer Rights, Washington, D.C.

11.14.13 **Homeland Threats and the FBI's Response**
James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C.

09.23.13 **Combating Human Trafficking**
Joseph S. Campbell, Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, Joint Statement with Anne C. Gannon, National Coordinator for Child Exploitation Prevention and Interdiction, Office of the Deputy Attorney General, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C.

06.19.13

foreign intelligence information collected in a criminal investigation with intelligence officials.

The information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the USA Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the USA Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the USA Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. Clarification of information sharing abilities, due in part to Section 203, eliminated that hesitation and allows agents to more openly work with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, our Field Offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships. Even Legal Attaches (Legats) notice improved relationships with intelligence agencies. If even a portion of the information sharing capabilities is allowed to 'sunset' or terminate, then the element of uncertainty could be re-introduced and agents will again hesitate and take the time necessary to seek clarification of complicated information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI must initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeiting goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as the Intelligence Community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity. In one such case, information from a criminal Title III and criminal investigation was passed to Counterterrorism, as well as intelligence community partners, because the subject of the criminal case had previously been targeted by other agencies. Information sharing permitted each agency to pool their information and resources to investigate the interplay of criminal and foreign intelligence activity.

In one instance, a terrorism case initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantities of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The operation resulted in the arrest, indictment and subsequent deportation of the subjects, Syed Mustajab Shah, Muhammed Afridi, and Ilyas Ali, from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda.

Criminal enterprises are also frequently involved in, allied with or otherwise rely on smuggling operations. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has identified smugglers who provide false travel documents to special interest aliens, deal with corrupt foreign officials, and financially support extremist organizations, as well as illegitimate and quasi-legitimate business operators in the United States, who not only use the services of illegal aliens, but are also actively involved in smuggling as well.

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case.

Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.C.

06.19.13 **Overview of FBI Biometrics Efforts**
Steven M. Martinez, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, Statement Before the House Committee on Oversight and Government Reform, Subcommittee on Government Operations, Washington, D.C.

06.13.13 **Addressing Diverse Threats to Our Nation While Preserving Civil Liberties**
Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the House Committee on the Judiciary, Washington, D.C.

06.12.13 **Cyber Security: Preparing for and Responding to the Enduring Threat**
Richard A. McFeely, Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, Federal Bureau of Investigation, Statement Before the Senate Appropriations Committee, Washington, D.C.

More

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

Section 204 is essentially a technical amendment. It clarifies that the law which governs the installation and use of pen registers and trap and trace devices will not interfere with certain foreign intelligence activities that fall outside the definition of "electronic surveillance" in the FISA statute. The provision also clarifies that the exclusivity provisions in Title 18 section 2511(2)(f) apply not only to the interception of wire and oral communications, but also to the interception of electronic communications.

Section 206 - Roving FISA Surveillance

With this provision, when a FISA target's actions have the effect of thwarting surveillance, such as by rapidly switching cell phones or even meeting venues, the Court can issue an order directing an as yet unknown cell phone carrier or other company to effect the authorized electronic surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order.

Section 206 has been extremely helpful especially with regard to international terrorism and foreign counterintelligence investigations where targets move quickly and often act evasively to avoid detection. Field Offices have observed counterintelligence targets change services for hard-line telephones and cell phones numerous times. The roving authority allows us to continuously monitor these targets without interruption. By minimizing the need to return to the court for additional authorizations, it also has allowed agents to more expeditiously conclude investigations.

In one case, a roving FISA on a subject's cellular telephone was approved for the subject of a counterintelligence investigation who, per the usage of tradecraft, is directed to change his cellular phone at regular intervals. The roving FISA allows us to continue coverage on all cell phones the subject obtains.

Section 207 - Extended Duration for Certain FISAs

Section 207 extends the standard duration for several categories of FISA orders. Before the enactment of the USA Patriot Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of ninety days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than 45 days, unless the target was a foreign power, in which case, the order could be issued for one year. This provision allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for ninety days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance may apply or extend for periods of 120 days, and renewal orders can be extended for up to one year.

Section 207 has led to reduced paperwork in certain categories of cases. In addition, it has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed agents to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail.

Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation.

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

Service providers have voluntarily provided information under this provision. Such disclosures often included both e-mail content and associated records. This provision has also been utilized to quickly locate kidnaping victims, protect children in child exploitation cases, and to quickly respond to bomb and death threats. Legats have also utilized this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing death or serious injury.

In one instance, an FBI Field Division received a bomb threat after hours. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, the FBI JTTF Agents began working with various communications providers to locate the caller. The caller was identified as a result of an emergency disclosure pursuant to this provision. An interview of the subject was conducted and the threat was determined to be non-credible by 11:00 a.m.

in a kidnaping case, a 14- year-old girl was abducted. As a result of the FBI's use of this provision, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours. This is but one example of how essential this provision is for child abduction cases.

Section 214 - FISA Pen/Trap Authority

The FBI may now obtain a FISA pen/trap and trace order from the court if "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications, comparable to the criminal pen/trap provision.

The results from these pen/trap orders often help agents to determine links between the subjects of different terrorism investigations, identify other unknown associates of the subject, discover contacts for potential assets, and develop the subject's personal profile. When pen/trap orders are quickly obtained, they allow agents to more quickly identify the associates tied to the subject of international terrorism investigations than if the agents were required to wait for service providers to respond to subpoenas for toll records, which can take several months. The old standard required more fact gathering to meet the threshold to obtain the pen/trap order, making this technique less effective and sometimes even preventing the use of this technique altogether if the window of opportunity was missed. The FISA pen/trap orders that have been obtained have been used on both terrorism and counterintelligence cases.

In one terrorism case, the only phone that the Field Office could prove was used by the subject was his associate's phone. Additionally, the Field Office had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the office may not have succeeded in obtaining the FISA pen/trap order. The standard established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations.

In another example, use of this section allowed FISA pen/trap authority based on the fact that information was likely to result in foreign intelligence information. This provision allowed the Field Office to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject, the organization and terrorism- related matters.

Section 215 - Access to Business Records under FISA

Section 215 changed the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records (i.e. hotels, motels, car and truck rentals) to include "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Obtaining business records is a longstanding law enforcement tool. Ordinary grand juries for years have issued subpoenas to all manner of businesses for records relevant to criminal investigations. Section 215 authorized the FISA Court to issue similar orders in national security investigations. It contains a number of safeguards that protect civil liberties. Section 215 requires FBI Agents to get a court order. Agents cannot use this authority unilaterally to compel any entity to turn over its records. In addition Section 215 has a narrow scope. It can only be used to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. It cannot be used to investigate ordinary crimes, or even domestic terrorism.

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The USA Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals that use and trade stolen credit card information). The group utilized a variety of methods to conceal their identities. The owner of the hacked computer was not aware of the misuse, and considered all individuals misusing its computers to be trespassers. The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of

could have identified the trespassers.

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 amended FISA to require a certification to the FISA Court that obtaining foreign intelligence gathering is "a significant purpose" of the FISA surveillance or search, rather than a "primary purpose" of such surveillance. Section 504 amended FISA to clarify that personnel involved in a foreign intelligence investigation can consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were intended to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their investigations at risk.

As stated above, FBI Field Offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision makes it clear that prosecutors can be involved in the earliest phases of an international terrorism investigation. AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

The ability to have criminal prosecutors involved in the earliest investigative phases of terrorism cases allows counterterrorism investigators to utilize the full selection of both intelligence and criminal investigative tools, enabling them to select and interchange these tools to meet the investigative demands of each particular case. Field Offices use criminal prosecution, or the threat thereof, in furtherance of the intelligence objective to disrupt and dismantle terrorism, towards the ultimate goal of preventing terrorist acts. One Field Office notes that if 218 were allowed to "sunset," its aggressive and effective investigative approach toward terrorism would be "severely crippled."

Section 220 - Search Warrants for Electronic Evidence

Section 220 of the USA Patriot Act enabled courts with jurisdiction over an investigation to issue a search warrant to compel the production of information held by a service provider located outside the district, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

The FBI routinely relies upon this provision when a search warrant is used to obtain the content of e-mail messages and other related information from Internet service providers (ISPs) in accordance with 18 U.S.C. § 2703.

Prior to the USA Patriot Act, if an investigator sought a search warrant to obtain the content of unopened e-mail from a service provider, the investigator was required to obtain this search warrant from a court in the jurisdiction where the service provider was located. To accomplish this, the case agent would brief an agent and prosecutor located in the ISP's jurisdiction on the facts of the case so that they might appear before the court and obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest ISPs are located in a few districts such as, the Northern District of California and the Eastern District of Virginia, these offices were faced with a substantial workload just to obtain search warrants for other offices.

While the USA Patriot Act maintained the legal standard of probable cause that must be met before the search warrant could be issued, it eliminated the additional bureaucratic paperwork necessary to obtain that warrant in a different jurisdiction than the investigation itself. This eliminated the need to involve additional agents and prosecutors located in the same jurisdiction as the ISP. Therefore, this provision expedites the process and minimizes the labor involved without altering the privacy protection afforded the e-mail and other associated records.

Field Offices repeatedly stated that this was very beneficial to quickly obtain information required in their investigations. The information obtained from these search warrants often leads to additional electronic evidence that is otherwise easily and quickly lost. Minimizing the time required to obtain the initial information from the ISPs is a significant asset to the investigations.

In the "Virginia Jihad" case, six subjects pled guilty and three were convicted of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. They received sentences ranging from a prison term of four years to life imprisonment. As a part of this case, court orders were issued to Internet Service Providers throughout the country to obtain information that resulted in valuable intelligence and criminal evidence used in the successful prosecution. Due to Section 220, all the court orders were issued by the district court where the prosecution occurred making the process much faster and more efficient.

This provision is regularly used in child pornography cases as agents obtain information from ISPs regarding those trading sexually exploitive images of children. This expedites the investigative process and minimizes the number of FBI, U.S. Attorney, and judicial personnel involved in the process, freeing them to more aggressively pursue investigative matters.

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the USA Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials

while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation by creating an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISA Court to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent of a foreign power, such as an international terrorist or spy. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies, to carry out such court orders. Prior to the passage of the USA Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISA Court under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay.

In an FBI Field Office, a case agent was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target was an espionage subject.

Section 213 - Delayed Notice Search Warrants

While not scheduled to sunset, the USA Patriot Act's delayed notice provision, Section 213, has been the subject of criticism and various legislative proposals. The FBI believes that Section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. It is important to note that delayed notice warrants were not created by the USA Patriot Act. Rather, the Act simply codified a common law practice recognized by courts across the country and created a uniform nationwide standard for the issuance of those warrants. The USA Patriot Act ensures that delayed notice search warrants are evaluated under the same criteria across the nation. Like any other search warrant, a delayed notice search warrant is issued by a federal judge only upon a showing that there is probable cause to believe that the property to be searched for or seized constitutes evidence of a criminal offense. A delayed notice warrant differs from an ordinary search warrant only in that the judge specifically authorizes the law enforcement officers executing the warrant to wait for a limited period of time before notifying the subject of the search that a search had been executed.

Delayed notice search warrants provide a crucial option to law enforcement and can only be issued if a federal judge finds that one of five tailored circumstances exists. The FBI has requested this authority in several cases. In most instances, the FBI seeks delayed notice when contemporaneous notice would reasonably be expected to cause serious jeopardy to an ongoing investigation.

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the USA Patriot Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address another area in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

Administrative Subpoenas

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and enforcement is difficult. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously, Section 215, which does not contain an emergency provision, may not be the most effective process to undertake. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal should provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the USA Patriot Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today. I am happy to answer any of your questions.